

**BURSOR & FISHER, P.A.**

Sarah N. Westcot (State Bar No. 264916)

701 Brickell Ave., Suite 2100

Miami, FL 33131-2800

Telephone: (305) 330-5512

Facsimile: (305) 676-9006

Email: [swestcot@bursor.com](mailto:swestcot@bursor.com)

*Counsel for Plaintiff*

**UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA**

J.S., individually and on behalf of all others  
similarly situated,

Plaintiff,

v.

SPRING FERTILITY HOLDINGS, LLC,

Defendant.

Case No. 5:24-cv-07374-EJD

**FIRST AMENDED CLASS ACTION  
COMPLAINT**

**JURY TRIAL DEMANDED**

1 Plaintiff J.S. (“Plaintiff”) brings this class action complaint on behalf of herself and all  
2 others similarly situated (the “Class Members”) against Defendant Spring Fertility Holdings, LLC  
3 (“Spring Fertility” or “Defendant”). Plaintiff brings this action based on personal knowledge of the  
4 facts pertaining to herself, and on information and belief as to all other matters, by and through the  
5 investigation of undersigned counsel.

### 6 **NATURE OF THE ACTION**

7 1. This is a class action brought on behalf of all patients who accessed and used  
8 www.springfertility.com (the “Website”) to book a consultation for fertility services.

9 2. Seeking fertility treatments often represents a deeply personal and emotionally  
10 taxing journey. The process can be fraught with physical discomfort, uncertainty, and a range of  
11 emotional responses, from hope and excitement to frustration and despair. The constant cycle of  
12 anticipation and disappointment can be emotionally exhausting, as patients grapple with the  
13 pressures of both medical outcomes and societal expectations.

14 3. Given these challenges, maintaining patient privacy is paramount. Fertility  
15 treatments are inherently personal, involving intimate details about an individual’s health,  
16 reproductive choices, and, often, their sexual orientation. The desire for privacy stems not only  
17 from the sensitivity of the medical information, but also from the emotional vulnerability that  
18 accompanies the process.

19 4. When seeking fertility treatment patients expect that their healthcare providers will  
20 maintain strict confidentiality and uphold the trust and respect that patients expect and need during  
21 such a vulnerable time.

22 5. Defendant knows this, promising its patients that “everything [] we do at each of our  
23 locations is focused on putting patients’ needs first[.]”<sup>1</sup> Despite that promise, Defendant aided,  
24 employed, agreed, and conspired with social media websites Meta Platforms, Inc. (“Facebook”) and  
25 LinkedIn Corporation (“LinkedIn”) to intercept sensitive and confidential personal and  
26 medical communications sent by patients seeking to book services with Spring Fertility through its  
27 website. This was a serious invasion of privacy divulging deeply personal aspects of an

28 <sup>1</sup> SPRING FERTILITY, <https://springfertility.com/>

1 individual's life. The interception of communications was particularly egregious because it  
2 included highly sensitive details including the specific type of fertility treatment sought, all without  
3 the patients' knowledge or consent.

4 6. Plaintiff brings this action for legal and equitable remedies resulting from these  
5 illegal actions.

## 6 **PARTIES**

7 7. Plaintiff J.S. is a California citizen who resides in Oakland, California. Plaintiff was  
8 in California when she booked a consultation for fertility services using the Website.

9 8. Plaintiff attended her consultation and received fertility services related to IVF  
10 treatment from Defendant Spring Fertility.

11 9. During the time Plaintiff used the Website, she maintained social media accounts  
12 with Facebook and LinkedIn. Plaintiff used the same device to access the Website and her  
13 Facebook and LinkedIn accounts. Subsequently, as a result of the conduct of Defendant, she  
14 received targeted advertisements on Facebook and LinkedIn relating to fertility services.

15 10. Pursuant to the systematic process described herein, Spring Fertility assisted  
16 Facebook and LinkedIn with intercepting Plaintiff's communications, including those that  
17 contained personally identifiable information ("PII"), protected health information (or "PHI").  
18 This includes information related to the specific fertility treatment she received with Spring  
19 Fertility. Defendant Spring Fertility assisted Facebook and LinkedIn's interceptions without  
20 Plaintiff's knowledge, consent, or express written authorization.

21 11. By failing to receive the requisite consent, Spring Fertility breached its duty of  
22 confidentiality and aided Facebook and LinkedIn in unlawfully intercepting Plaintiff's PII and PHI.

23 12. Such acts are egregious violations of Plaintiff's right to privacy.

24 13. Defendant Spring Fertility Holdings, LLC is incorporated in Delaware with its  
25 principal place of business in San Francisco, California. Defendant Spring Fertility owns and  
26 operates the Website [www.springfertility.com](http://www.springfertility.com). Defendant Spring Fertility provides fertility  
27 services and treatments for consumers.<sup>2</sup> Defendant Spring Fertility embedded tracking software

28 <sup>2</sup> SPRING FERTILITY, <https://springfertility.com/resources-faq/#infertility-faq>.

1 known as the Facebook Tracking Pixel and LinkedIn Insight Tag on its Website, as described in  
2 more detail below. Defendant Spring Fertility embedded these tracking technologies on its  
3 Website for advertising purposes.

#### 4 **JURISDICTION AND VENUE**

5 14. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. §  
6 1331 because it arises under a law of the United States (the Electronic Communications Privacy  
7 Act, 18 U.S.C. § 2511). This Court also has supplemental jurisdiction over Plaintiff's state law  
8 claims under 28 U.S.C. § 1367. Further, this action is a putative class action, and Plaintiff alleges  
9 that at least 100 people comprise the proposed class, that the combined claims of the proposed  
10 class members exceed \$5,000,000 exclusive of interest and costs, and that at least one member of  
11 the proposed class is a citizen of a state different from at least one defendant.

12 15. This Court has personal jurisdiction over the parties because Plaintiff resides in  
13 California, is a California citizen, and submits to the jurisdiction of the Court. Further, Defendant  
14 has, at all times relevant hereto, systematically and continually conducted business in California,  
15 including within this District, and intentionally availed itself of the benefits and privileges of the  
16 California consumer market through the promotion, marketing, and sale of its services to residents  
17 within this District and throughout California. Additionally, Plaintiff, while in California, booked  
18 a consultation for fertility services at one of Defendant Spring Fertility's California locations using  
19 the Website.

20 16. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant  
21 transacts significant business within this District and Plaintiff resides in this District.

#### 22 **FACTUAL ALLEGATIONS**

##### 23 **A. Background of the California Information Privacy Act ("CIPA")**

24 17. The CIPA, California Penal Code Section 630, *et seq.*, prohibits aiding or permitting  
25 another person to willfully—and without the consent of all parties to a communication—read or  
26 learn the contents or meaning of any message, report, or communication while the same is in transit  
27 or passing over any wire, line, or cable, or is being sent from or received at any place within  
28 California.

1           18. To establish liability under California Penal Code Section 631(a), a plaintiff need  
2 only establish that the defendant, “by means of any machine, instrument, or contrivance, or in any  
3 other manner,” does any of the following:

4           Intentionally taps, or makes any unauthorized connection, whether physically,  
5 electrically, acoustically, inductively or otherwise, with any telegraph or telephone  
6 wire, line, cable, or instrument, including the wire, line, cable, or instrument of any  
internal telephonic communication system,

7           Or

8           Willfully and without the consent of all parties to the communication, or in any  
9 unauthorized manner, reads or attempts to read, or to learn the contents or meaning  
10 of any message, report, or communication while the same is in transit or passing over  
any wire, line or cable, or is being sent from, or received at any place within this state,

11          Or

12          Aids, agrees with, employs, or conspires with any person or persons to unlawfully do,  
13 or permit, or cause to be done any of the acts or things mentioned above in this section.

14          19. Section 631(a)’s applicability is not limited to phone lines, but also applies to “new  
15 technologies” such as computers, the internet, and email. *See Matera v. Google Inc.*, 2016 WL  
16 8200619, at \*21 (N.D. Cal. Aug. 12, 2016) (the CIPA applies to “new technologies” and must be  
17 construed broadly to effectuate its remedial purpose of protecting privacy); *Bradley v. Google, Inc.*,  
18 2006 WL 3798134, at \*5–6 (N.D. Cal. Dec. 22, 2006) (the CIPA governs “electronic  
19 communications”); *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589, 607–08 (9th  
20 Cir. 2020) (reversing dismissal of CIPA and common law privacy claims based on Facebook’s  
21 collection of consumers’ internet browsing history).

22          20. Plaintiff and Class Members may seek injunctive relief and statutory damages of  
23 \$5,000 per violation under the CIPA. Cal. Penal Code § 637.2.

24           **B. Background of the California Confidentiality of Medical  
Information Act (“CMIA”)**

25          21. Under the CMIA a “provider of health care . . . shall not disclose medical  
26 information regarding a patient of the provider of health care . . . without first obtaining an  
27  
28

1 authorization, except as provided in subdivision (b) or (c).” Cal. Civ. Code § 56.10(a).<sup>3</sup> “An  
2 authorization for the release of medical information . . . shall be valid if it:

3 (1) Is handwritten or is in a typeface no smaller than 14-point type.

4 (2) Is clearly separate from any other language present on the same page and is  
5 executed by a signature that serves no other purpose than to execute the authorization.

6 (3) Is signed . . . and dated . . .

7 (4) States the specific uses and limitations on the types of medical information to be  
8 disclosed.

9 (5) States the name or functions of the provider of health care, health care service  
10 plan, pharmaceutical company, or contractor that may disclose the medical  
information.

11 (6) States the name or functions of the persons or entities authorized to receive the  
12 medical information.

13 (7) States the specific uses and limitations on the use of the medical information by  
14 the persons or entities authorized to receive the medical information.

15 (8) States an expiration date or event . . . .

16 (9) Advises the person signing the authorization of the right to receive a copy of the  
authorization.”<sup>4</sup>

17 22. Moreover, a health care provider that maintains information for purposes covered by  
18 the CMIA is liable for negligent disclosures that arise as the result of an affirmative act—such as  
19 implementing a system that records and discloses online patients’ personally identifiable  
20 information and PHI. Cal. Civ. Code § 56.36(c).<sup>5</sup> Similarly, if a negligent release occurs and  
21

22 <sup>3</sup> Subdivisions (b) and (c) are not relevant to this case but permit the disclosure of medical  
23 information in situations where a government investigation or lawsuit is taking place. For example,  
24 Defendant Spring Fertility could bypass the authorization requirement if patient medical information  
was requested pursuant to a lawful court order or by a party to a proceeding before a court or  
administrative agency pursuant to a subpoena. *See* Cal. Civ. Code §§ 56.10(b)(3) & 56.10(b)(6).

25 <sup>4</sup> Cal. Civ. Code § 56.11(b).

26 <sup>5</sup> “Every provider of health care . . . who creates, maintains, preserves, stores, abandons, destroys,  
27 or disposes of medical information shall do so in a manner that preserves the confidentiality of the  
information contained therein. Any provider of health care . . . who negligently creates, maintains,  
28 preserves, stores, abandons, destroys, or disposes of medical information shall be subject to the  
remedies and penalties provided under subdivisions (b) and (c) of Section 56.36.” Cal. Civ. Code §  
56.101(a).

1 medical information concerning a patient is improperly viewed or otherwise accessed, the  
2 individual need not suffer actual damages to sue. Cal. Civ. Code § 56.36(b). The California Third  
3 District Court of Appeal emphasized this in *Sutter Health*:

4 In addition to any other remedies available at law, any individual may  
5 bring an action against any person or entity who has negligently  
6 released confidential information or records concerning him or her in  
7 violation of this part, for either or both of the following: [¶] (1) . . .  
8 nominal damages of one thousand dollars (\$1,000). In order to recover  
under this paragraph, it shall not be necessary that the plaintiff suffered  
or was threatened with actual damages. [¶] (2) The amount of actual  
damages, if any, sustained by the patient.<sup>6</sup>

9 **C. Health Information Is Sensitive And Confidential**

10 23. Defendant assisted Facebook and LinkedIn, two of the largest data and technology  
11 companies in the world, with intercepting information that is sensitive, confidential, and personally  
12 identifiable.

13 24. Under federal law, a healthcare provider may not disclose personally identifiable  
14 information (“PII”) or protected health information (“PHI”) without the patient’s express written  
15 authorization.<sup>7</sup> In this case, PHI includes, but is not necessarily limited to, information pertaining  
16 to fertility treatment.

17 25. The United States Department of Health and Human Services (“HHS”) has  
18 established a national standard, known as the HIPAA Privacy Rule, to explain the duties healthcare  
19 providers owe to their patients. “The Rule requires appropriate safeguards to protect the privacy of  
20 [PHI] and sets limits and conditions on the uses and disclosures that may be made of such  
21 information without an individual’s authorization.”<sup>8</sup>  
22  
23  
24

25 <sup>6</sup> *Sutter Health v. Superior Ct.*, 227 Cal. App. 4th 1546, 1551 (2014) (quoting Cal. Civ. Code §  
26 56.36(b)).

27 <sup>7</sup> HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502, 165.508(a), 164.514(b)(2)(i).

28 <sup>8</sup> U.S. Dept. of Health and Human Services, <https://www.hhs.gov/hipaa/for-professionals/privacy/index.html>.

1           26.     A healthcare provider violates the HIPAA Privacy Rule if it knowingly and in  
2 violation of 42 U.S.C. §§ 1320d-d9 (“Part C”): “(1) uses of causes to be used a unique health  
3 identifier; [or] (2) obtains individually identifiable health information relating to an individual.”<sup>9</sup>

4           27.     The statute states that an entity “shall be considered to have obtained or disclosed  
5 individually identifiable health information in violation of [Part C] if the information is maintained  
6 by a covered entity...and the individual obtained or disclosed such information without  
7 authorization.” *Id.*

8           28.     The criminal and civil penalties imposed by 42 U.S.C. § 1320d-6 apply directly to  
9 Defendant because it knowingly disclosed individually identifiable health information relating to  
10 its patients.

11          29.     Defendant further failed to comply with other HIPAA safeguard regulations as  
12 follows:

- 13           a.     Failing to ensure the confidentiality and integrity of electronic PHI that Defendant  
14                 created, received, maintained and transmitted in violation of 45 C.F.R. Section  
15                 164.306(a)(1);
- 16           b.     Failing to implement policies and procedures to prevent, detect, contain and correct  
17                 security violations in violation of 45 C.R.F. Section 164.308(a)(1);
- 18           c.     Failing to identify and respond to suspected or known security incidents and  
19                 mitigate harmful effects of security incidents known to Defendant in violation of 45  
20                 C.F.R. Section 164.308(a)(6)(ii);
- 21           d.     Failing to protect against reasonably anticipated threats or hazards to the security or  
22                 integrity of electronic PHI in violation of 45 C.F.R. Section 306(a)(2);
- 23           e.     Failing to protect against reasonably anticipated uses of disclosures of electronic  
24                 PHI not permitted under privacy rules pertaining to individually identifiable health  
25                 information in violation of 45 C.F.R. Section 164.306(a)(3); and

26  
27  
28           <sup>9</sup> 42 U.S.C. § 1320d-6.



1 f. Failing to design, implement and enforce policies and procedures that would  
2 establish physical and administrative safeguards to reasonably safeguard PHI in  
3 violation of 45 C.F.R. Section 164.530(c).

4 30. Health care organizations regulated under HIPAA, like Defendant, may use third-  
5 party tracking tools in a limited way to perform analysis on data key to operations. They are not  
6 permitted, however, to use these tools in a way that may expose patients' PHI to vendors (as shown  
7 below). As explained by a statement published by the HHS:

8 Regulated entities [those to which HIPAA applies] are not permitted  
9 to use tracking technologies in a manner that would result in  
10 impermissible disclosures of PHI to tracking technology vendors or  
11 any other violations of the HIPAA Rules. **For example, disclosures  
12 of PHI to tracking technology vendors for marketing purposes,  
without individuals' HIPAA-compliant authorizations, would  
constitute impermissible disclosures.**<sup>10</sup>

13 31. The Bulletin discusses the types of harm that disclosure may cause to the patient:  
14 An impermissible disclosure of an individual's PHI not only violates  
15 the Privacy Rule but also may result in a wide range of additional  
16 harms to the individual or others. For example, an impermissible  
17 disclosure of PHI may result in identity theft, financial loss,  
18 discrimination, stigma, mental anguish, or other serious negative  
19 consequences to the reputation, health, or physical safety of the  
20 individual or to others identified in the individual's PHI. Such  
21 disclosures can reveal incredibly sensitive information about an  
22 individual, including diagnoses, frequency of visits to a therapist or  
23 other health care professionals, and where an individual seeks  
24 medical treatment. While it has always been true that regulated  
25 entities may not impermissibly disclose PHI to tracking technology  
26 vendors, **because of the proliferation of tracking technologies  
collecting sensitive information, now more than ever, it is critical  
for regulated entities to ensure that they disclose PHI only as  
expressly permitted or required by the HIPAA Privacy Rule.**<sup>11</sup>

27 32. Plaintiff and Class Members face exactly the risks about which the government  
28 expresses concern. Defendant's unlawful conduct resulted in third parties intercepting information

26 <sup>10</sup> HHS.gov, USE OF ONLINE TRACKING TECHNOLOGIES BY HIPAA COVERED ENTITIES AND  
27 BUSINESS ASSOCIATES (THE "BULLETIN") (EMPHASIS ADDED), [https://www.hhs.gov/hipaa/for-  
professionals/privacy/guidance/hipaa-online-tracking/index.html](https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html).

28 <sup>11</sup> *Id.* (emphasis added).

1 regarding Plaintiff and Class Members’ fertility appointments and treatments on Defendant’s  
2 Website.

3 33. The Bulletin goes on to make clear how broad the government’s view of protected  
4 information is. It explains:

5 This information might include an individual’s medical record  
6 number, home or email address, or dates of appointments, as well as  
7 an individual’s IP address or geographic location, medical device  
8 IDs, or any unique identifying code.<sup>12</sup>

9 34. Crucially, the Bulletin continues:

10 All such [individually identifiable health information (“IIHI”)]  
11 collected on a regulated entity’s website or mobile app generally is  
12 PHI, even if the individual does not have an existing relationship  
13 with the regulated entity and even if the IIHI, such as IP address or  
14 geographic location, does not include specific treatment or billing  
15 information like dates and types of health care services. This is  
16 because, when a regulated entity collects the individual’s IIHI  
17 through its website or mobile app, the information connects the  
18 individual to the regulated entity (i.e., it is indicative that the  
19 individual has received or will receive health care services or benefits  
20 from the covered entity), and thus **relates to the individual’s past,  
21 present, or future health or health care** or payment for care.<sup>13</sup>

22 35. Then, in July 2022, the Federal Trade Commission (“FTC”) and the Department of  
23 Health and Human Services (“HHS”) issued a joint press release warning regulated entities about  
24 the privacy and security risks arising from the use of online tracking technologies:

25 The Federal Trade Commission and the U.S. Department of Health  
26 and Human Services’ Office for Civil Rights (OCR) are cautioning  
27 hospitals and telehealth providers [regulated entities] about the  
28 privacy and security risks related to the use of online tracking  
technologies integrated into their websites or mobile apps that may  
be impermissibly disclosing consumers’ sensitive personal health  
data to third parties.

“When consumers visit a hospital’s [regulated entity’s] website or  
seek telehealth services, they should not have to worry that their most  
private and sensitive health information may be disclosed to  
advertisers and other unnamed, hidden third parties,” said Samuel  
Levine, Director of the FTC’s Bureau of Consumer Protection. “The

---

<sup>12</sup> *Id.* (emphasis added).

<sup>13</sup> *Id.* (emphasis added).

1 FTC is again serving notice that companies need to exercise extreme  
2 caution when using online tracking technologies and that we will  
3 continue doing everything in our powers to protect consumers' health  
information from potential misuse and exploitation."

4 "Although online tracking technologies can be used for beneficial  
5 purposes, patients and others should not have to sacrifice the privacy  
of their health information when using a hospital's [regulated  
entity's] website," said Melanie Fontes Rainer, OCR Director.

6 "OCR continues to be concerned about impermissible disclosures of  
7 health information to third parties and will use all of its resources to  
address this issue."

8 The two agencies sent the joint letter to approximately 130 [regulated  
9 entities] hospital systems and telehealth providers to alert them about  
the risks and concerns about the use of technologies, such as the  
10 Meta/Facebook pixel and Google Analytics, that can track a user's  
online activities. These tracking technologies gather identifiable  
11 information about users, usually without their knowledge and in  
ways that are hard for users to avoid, as users interact with a website  
12 or mobile app.

13 In their letter, both agencies reiterated the risks posed by the  
14 unauthorized disclosure of an individual's personal health  
information to third parties. For example, the disclosure of such  
15 information could reveal sensitive information including health  
conditions, diagnoses, medications, medical treatments, frequency of  
16 visits to health care professionals, and where an individual seeks  
medical treatment.<sup>14</sup>

17 36. The FTC is unequivocal in its stance. The FTC has specifically informed healthcare  
18 companies, like Defendant, that they should not use tracking technologies to collect sensitive  
19 health information and disclose it to third party advertising platforms without informed consent:

20 The FTC Act prohibits companies and individuals from engaging in  
21 unfair or deceptive acts or practices in or affecting commerce. This  
means you must ensure your health data practices aren't substantially  
22 injuring consumers, including by invading their privacy.

23 For instance, BetterHelp, GoodRx, and Premom make clear that  
24 disclosing consumers' health information for advertising without  
their affirmative express consent may be an unfair practice.

25  
26 <sup>14</sup> Federal Trade Commission, *FTC and HHS Warn Hospital Systems and Telehealth Providers*  
27 *about Privacy and Security Risks from Online Tracking Technologies*, July 20, 2023,  
28 <https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking>. (emphasis added).

1 [I]f you use behind-the-scenes tracking technologies that share  
2 consumers' sensitive health data in contradiction of your privacy  
promises, that's a violation of the FTC Act.<sup>15</sup>

3 37. Therefore, Defendant's conduct, as described herein, is directly contrary to federal  
4 law and the clear pronouncements by the FTC and HHS.

5 **D. Facebook's Platform and Business Tools**

6 38. Facebook describes itself as a "real identity platform,"<sup>16</sup> meaning users are allowed  
7 only one account and must share "the name they go by in everyday life."<sup>17</sup> To that end, when  
8 creating an account, users must provide their first and last name, along with their birthday and  
9 gender.<sup>18</sup>

10 39. In 2023, Facebook generated over \$134 billion in revenue.<sup>19</sup> With respect to the  
11 apps offered by Facebook, substantially all of Facebook's revenue is generated by selling  
12 advertising space.<sup>20</sup>

13 40. Facebook sells advertising space by highlighting its ability to target users.<sup>21</sup>  
14 Facebook can target users effectively because it surveils user activity on and off its site.<sup>22</sup> This  
15 allows Facebook to make inferences about users beyond what they explicitly disclose, like their  
16  
17

18 <sup>15</sup> [https://www.ftc.gov/business-guidance/resources/collecting-using-or-sharing-consumer-health-](https://www.ftc.gov/business-guidance/resources/collecting-using-or-sharing-consumer-health-information-look-hipaa-ftc-act-health-breach)  
19 [information-look-hipaa-ftc-act-health-breach](https://www.ftc.gov/business-guidance/resources/collecting-using-or-sharing-consumer-health-information-look-hipaa-ftc-act-health-breach)

20 <sup>16</sup> Sam Schechner & Jeff Horwitz, *How Many Users Does Facebook Have? The Company*  
21 *Struggles to Figure It Out*, WALL ST. J. (Oct. 21, 2021, 4:05 PM),  
[https://www.wsj.com/articles/how-many-users-does-facebook-have-the-company-struggles-to-](https://www.wsj.com/articles/how-many-users-does-facebook-have-the-company-struggles-to-figure-it-out-11634846701)  
figure-it-out-11634846701.

22 <sup>17</sup> FACEBOOK, COMMUNITY STANDARDS, PART IV INTEGRITY AND AUTHENTICITY,  
[https://www.facebook.com/communitystandards/integrity\\_authenticity](https://www.facebook.com/communitystandards/integrity_authenticity).

23 <sup>18</sup> FACEBOOK, SIGN UP, <https://www.facebook.com>.

24 <sup>19</sup> FACEBOOK, META REPORTS FOURTH QUARTER AND FULL YEAR 2023 RESULTS; INITIATES  
25 QUARTERLY DIVIDEND, [https://s21.q4cdn.com/399680738/files/doc\\_news/Meta-Reports-Fourth-](https://s21.q4cdn.com/399680738/files/doc_news/Meta-Reports-Fourth-Quarter-and-Full-Year-2023-Results-Initiates-Quarterly-Dividend-2024.pdf)  
Quarter-and-Full-Year-2023-Results-Initiates-Quarterly-Dividend-2024.pdf at 8.

26 <sup>20</sup> *Id.*

27 <sup>21</sup> FACEBOOK, WHY ADVERTISE ON FACEBOOK, INSTAGRAM AND OTHER META TECHNOLOGIES,  
<https://www.facebook.com/business/help/205029060038706>.

28 <sup>22</sup> FACEBOOK, ABOUT META PIXEL,  
<https://www.facebook.com/business/help/742478679120153?id=1205376682832142>.

1 “interests,” “behavior,” and “connections.”<sup>23</sup> Facebook compiles this information into a  
2 generalized dataset called “Core Audiences,” which allows advertisers to reach precise audiences  
3 based on specified targeting types.<sup>24</sup>

4 41. Advertisers can also build “Custom Audiences.”<sup>25</sup> Custom Audiences enables  
5 advertisers to reach “people who have already shown interest in [their] business, whether they’re  
6 loyal customers or people who have used [their] app or visited [their] website.”<sup>26</sup> With Custom  
7 Audiences, advertisers can target existing customers directly and build “Lookalike Audiences,”  
8 which “leverage[] information such as demographics, interests and behaviors from your source  
9 audience to find new people who share similar qualities.”<sup>27</sup> Unlike Core Audiences, advertisers  
10 can build Custom Audiences and Lookalike Audiences only if they first supply Facebook with the  
11 underlying data. They can do so through two mechanisms: (1) by manually uploading contact  
12 information for customers or (2) by utilizing Facebook’s “Business Tools.”<sup>28</sup>

13 42. As Facebook puts it, the Business Tools “help website owners and publishers, app  
14 developers, and business partners, including advertisers and others, integrate with [Facebook],  
15 understand and measure their products and services, and better reach and serve people who might  
16 be interested in their products and services.”<sup>29</sup> Put more succinctly, Facebook’s Business Tools are  
17 bits of code that advertisers can integrate into their websites, mobile applications, and servers,  
18 thereby enabling Facebook to intercept and collect user activity on those platforms.

19 43. The Business Tools are automatically configured to capture certain data, like when a

---

20 <sup>23</sup> FACEBOOK, AD TARGETING: HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS,  
21 <https://www.facebook.com/business/ads/ad-targeting>.

22 <sup>24</sup> FACEBOOK, <https://www.facebook.com/business/news/Core-Audiences>.

23 <sup>25</sup> FACEBOOK, ABOUT CUSTOM AUDIENCES,  
24 <https://www.facebook.com/business/help/744354708981227?id=2469097953376494>.

25 <sup>26</sup> FACEBOOK, AUDIENCE AD TARGETING, <https://www.facebook.com/business/ads/ad-targeting>.

26 <sup>27</sup> FACEBOOK, ABOUT LOOKALIKE AUDIENCES,  
27 <https://www.facebook.com/business/help/164749007013531?id=401668390442328>.

28 <sup>28</sup> FACEBOOK, CREATE A CUSTOMER LIST CUSTOM AUDIENCE,  
<https://www.facebook.com/business/help/170456843145568?id=2469097953376494>; FACEBOOK,  
CREATE A WEBSITE CUSTOM AUDIENCE,  
<https://www.facebook.com/business/help/1474662202748341?id=2469097953376494>.

<sup>29</sup> FACEBOOK, THE META BUSINESS TOOLS, <https://www.facebook.com/help/331509497253087>.

1 user visits a webpage, that webpage’s Universal Resource Locator (“URL”) and metadata, or when  
2 a user downloads a mobile application or makes a purchase.<sup>30</sup> Facebook’s Business Tools can also  
3 track other events. Facebook offers a menu of “standard events” from which advertisers can  
4 choose, including what content a visitor views or purchases.<sup>31</sup> Advertisers can even create their  
5 own tracking parameters by building a “custom event.”<sup>32</sup>

6 44. One such Business Tool is the Facebook Tracking Pixel. Facebook offers this piece  
7 of code to advertisers, like Spring Fertility, to integrate into their website. As the name implies, the  
8 Facebook Tracking Pixel “tracks the people and type of actions they take.”<sup>33</sup> When a user accesses  
9 a website hosting the Facebook Tracking Pixel, Facebook’s software script surreptitiously directs  
10 the user’s browser to contemporaneously send a separate message to Facebook’s servers. This  
11 second secret and contemporaneous transmission contains the original GET request sent to the host  
12 website, along with additional data that the Facebook Tracking Pixel is configured to collect. This  
13 transmission is initiated by Facebook code and concurrent with the communications with the host  
14 website. At relevant times, two sets of code were thus automatically run as part of the browser’s  
15 attempt to load and read Defendant’s Website—Defendant’s own code and Facebook’s embedded  
16 code.

17 45. Defendant chose to include the Facebook Tracking Pixel on its Website.

18 46. Facebook’s own documentation makes clear how extensively the Facebook  
19 Tracking Pixel tracks private information. It describes the Facebook Tracking Pixel as code that  
20 Facebook’s business customers can put on their website to “[m]ake sure your ads are shown to the

21 <sup>30</sup> See FACEBOOK, META FOR DEVELOPERS: META PIXEL, ADVANCED,  
22 <https://developers.facebook.com/docs/meta-pixel/advanced/>; see also FACEBOOK, BEST PRACTICES  
23 FOR META PIXEL SETUP,  
24 <https://www.facebook.com/business/help/218844828315224?id=1205376682832142>; FACEBOOK,  
25 META FOR DEVELOPERS: MARKETING API - APP EVENTS API,  
26 <https://developers.facebook.com/docs/marketing-api/app-event-api/>.

27 <sup>31</sup> FACEBOOK, SPECIFICATIONS FOR META PIXEL STANDARD EVENTS,  
28 <https://www.facebook.com/business/help/402791146561655?id=1205376682832142>.

<sup>32</sup> FACEBOOK, ABOUT STANDARD AND CUSTOM WEBSITE EVENTS,  
<https://www.facebook.com/business/help/964258670337005?id=1205376682832142>; see also  
FACEBOOK, META FOR DEVELOPERS: MARKETING API – APP EVENTS API,  
<https://developers.facebook.com/docs/marketing-api/app-event-api/>.

<sup>33</sup> FACEBOOK, RETARGETING, <https://www.facebook.com/business/goals/retargeting>.

1 right people[] [and] *[find . . . people who have visited a specific page or taken a desired action on*  
2 *your website*” (emphasis added).<sup>34</sup>

3 47. Facebook instructs such business customers that:

4 Once you’ve set up the [Facebook Tracking] Pixel, *the pixel will log when someone*  
5 *takes an action on your website*. Examples of actions include adding an item to their  
6 shopping cart or making a purchase. *The Pixel receives these actions, or events,*  
7 which you can view on your [Facebook Tracking] Pixel page in Events Manager.  
8 From there, you’ll be able to see the actions that your customers take. *You’ll also*  
9 *have options to reach those customers again through future Meta ads*.<sup>35</sup>

10 48. Of course, in healthcare, it is medical specialists that users “add to their shopping  
11 cart.” They book fertility consultations rather than make purchases.

12 49. The Facebook Tracking Pixel code enables Facebook not only to help Defendant  
13 with advertising to its own patients outside the Website, but also includes individual patients  
14 among groups targeted by *other* Facebook advertisers relating to the conditions about which  
15 patients communicated on Defendant’s Website.

16 50. Facebook’s Business Help Center explains:

17 Meta *uses event data to show ads to people who are likely to be interested in them*.  
18 One type of marketing data is website events, which are *actions that people take on*  
19 *your website*.<sup>36</sup>

20 51. In other words, Facebook sells advertising space by highlighting its ability to target  
21 users.<sup>37</sup> Facebook can target users so effectively because it surveils user activity both on and off its  
22 site.<sup>38</sup> This allows Facebook to make inferences about users beyond what they explicitly disclose,  
23 like their “interests,” “behaviors,” and connections.<sup>39</sup>

24 52. An example illustrates how the Facebook Tracking Pixel works. Take an individual  
25 who, at relevant times, navigated to Defendant’s Website and clicked on a link to book a fertility

26 <sup>34</sup> META, ABOUT META PIXEL,  
27 <https://www.facebook.com/business/help/742478679120153?id=1205376682832142>.

28 <sup>35</sup> *Id.* (emphasis added).

<sup>36</sup> META, ABOUT STANDARD AND CUSTOM WEBSITE EVENTS,  
<https://www.facebook.com/business/help/964258670337005?id=1205376682832142> (emphasis  
added).

<sup>37</sup> META, WHY ADVERTISE ON FACEBOOK, INSTAGRAM AND OTHER META TECHNOLOGIES,  
<https://www.facebook.com/business/help/205029060038706> (last visited May 21, 2024).

<sup>38</sup> META, ABOUT META PIXEL,  
<https://www.facebook.com/business/help/742478679120153?id=1205376682832142>.

<sup>39</sup> META, AD TARGETING: HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS,  
<https://www.facebook.com/business/ads/ad-targeting>.

1 consultation. When that link was clicked, the individual's browser sent a GET request to  
2 Defendant's server requesting that server to load the particular webpage. As a result of  
3 Defendant's use of the Facebook Tracking Pixel, Facebook's embedded code, written in  
4 JavaScript, sent secret instructions back to the individual's browser, without alerting the individual  
5 that this was happening. Facebook caused the browser to secretly duplicate the communication  
6 with Defendant, transmitting it to Facebook's servers, alongside additional information that  
7 transcribed the communication's content and the individual's identity.

8 53. After collecting and intercepting the information described in the preceding  
9 paragraph, Facebook processed, analyzed, and assimilated it into datasets like Core Audiences and  
10 Custom Audiences.

#### 11 **E. LinkedIn's Platform and Business Tools**

12 54. LinkedIn markets itself as "the world's largest professional network on the  
13 internet[.]"<sup>40</sup> But LinkedIn is no longer simply a tool to help users find jobs or expand their  
14 professional network. LinkedIn has moved into the marketing and advertising space, and boasts of  
15 its ability to allow potential advertisers to "[r]each 1 billion+ professionals around the world" via  
16 its Marketing Solutions services.<sup>41</sup> Recently, LinkedIn was projected as being responsible for  
17 "roughly 0.9 percent of the global ad revenue" which included approximately \$5.91 billion in  
18 advertising revenue in 2022.<sup>42</sup>

19 55. According to LinkedIn, "[t]argeting is a foundational element of running a  
20 successful advertising campaign — [g]etting your targeting right leads to higher engagement, and  
21 ultimately, higher conversion rates."<sup>43</sup> Targeting refers to ensuring that advertisements are  
22 targeted to, and appear in front of, the target demographic for an advertisement. To that end,

23  
24 <sup>40</sup> LINKEDIN, WHAT IS LINKEDIN AND HOW CAN I USE IT?,  
<https://www.linkedin.com/help/linkedin/answer/a548441#>.

25 <sup>41</sup> LINKEDIN, MARKETING SOLUTIONS, <https://business.linkedin.com/marketing-solutions>.

26 <sup>42</sup> Valentina Dencheva, *LinkedIn annual ad revenue 2017-2027*, STATISTA (Dec. 12, 2023),  
<https://www.statista.com/statistics/275933/linkedins-advertising-revenue>.

27 <sup>43</sup> LINKEDIN, REACH YOUR AUDIENCE: TARGETING ON LINKEDIN, p.3,  
28 <https://business.linkedin.com/content/dam/me/business/en-us/marketing-solutions/resources/pdfs/linkedin-targeting-playbook-v3.pdf>.



1 LinkedIn's Marketing Solutions services allow potential advertisers to "[b]uild strategic  
2 campaigns" targeting specific users.<sup>44</sup> LinkedIn's "marketing solutions allow advertisers to select  
3 specific characteristics to help them reach their ideal audience. The ads [users] see on LinkedIn are  
4 then targeted to provide content relevant to [the users]."<sup>45</sup>

5 56. As a result of its activities and operation of the LinkedIn Insight Tag, LinkedIn is  
6 able to make extremely personal inferences about individuals' demographics, intent, behavior,  
7 engagement, interests, buying decisions, and more.<sup>46</sup>

8 57. The personal information and communications obtained by LinkedIn are used to  
9 fuel various services offered via LinkedIn's Marketing Solutions including Ad Targeting, Matched  
10 Audiences, Audience Expansion, and LinkedIn Audience Network.<sup>47</sup>

11 58. Such information is extremely valuable to marketers and advertisers because the  
12 inferences derived from users' personal information and communications allows marketers and  
13 advertisers, including healthcare providers and insurance companies, to target potential  
14 customers.<sup>48</sup>

---

17 <sup>44</sup> LINKEDIN, *supra* note 33.

18 <sup>45</sup> LINKEDIN, LINKEDIN ADS AND MARKETING SOLUTIONS,  
<https://www.linkedin.com/help/lms/answer/a421454>.

19 <sup>46</sup> See LINKEDIN, MARKETING SOLUTIONS, [https://business.linkedin.com/marketing-](https://business.linkedin.com/marketing-solutions/audience)  
20 [solutions/audience](https://business.linkedin.com/marketing-solutions/audience) ("Target audiences through demographic marketing[,] "Zero in on intent,  
behavior, engagement, interests, and more[,] and "Reach the LinkedIn audience involved in the  
buying decision").

21 <sup>47</sup> See *id.*

22 <sup>48</sup> LINKEDIN, PRIVACY POLICY, <https://www.linkedin.com/legal/privacy-policy> ("We serve you  
23 tailored ads both on and off our Services. We offer you choices regarding personalized ads, but you  
cannot opt-out of seeing other ads."); LINKEDIN, ACCOUNT TARGETING,  
24 <https://business.linkedin.com/marketing-solutions/ad-targeting> ("Target your ideal customer based  
on traits like their job title, company name or industry, and by professional or personal interests");  
25 LINKEDIN, EXAMPLES OF TRENDING AND BEST-IN-CLASS HEALTHCARE CAMPAIGNS AND CONTENT,  
p.6, [https://business.linkedin.com/content/dam/me/business/en-us/marketing-solutions/healthcare-](https://business.linkedin.com/content/dam/me/business/en-us/marketing-solutions/healthcare-microsite/resources/lkin-lms-sales-healthcare-campaigns-trending-content-Jan2023.pdf)  
26 [microsite/resources/lkin-lms-sales-healthcare-campaigns-trending-content-Jan2023.pdf](https://business.linkedin.com/content/dam/me/business/en-us/marketing-solutions/healthcare-microsite/resources/lkin-lms-sales-healthcare-campaigns-trending-content-Jan2023.pdf) ("BD  
zeroed in on the end-benefit with a 30 second video introducing their PIVO needle-free blood  
collection device to potential customers."); LINKEDIN, HEALTHCARE SOCIAL MEDIA STRATEGIES FOR  
27 2023, p.1, [https://business.linkedin.com/content/dam/me/business/en-us/marketing-](https://business.linkedin.com/content/dam/me/business/en-us/marketing-solutions/healthcare-microsite/resources/hc-social-media-trends.pdf)  
28 [solutions/healthcare-microsite/resources/hc-social-media-trends.pdf](https://business.linkedin.com/content/dam/me/business/en-us/marketing-solutions/healthcare-microsite/resources/hc-social-media-trends.pdf) (listing "potential customers"  
as "Common audiences" for insurance sector).

1           59. For example, through the use of LinkedIn’s Audience Network, marketers and  
2 advertisers are able to expand their reach and advertise on sites other than LinkedIn to “reach  
3 millions of professionals across multiple touchpoints.”<sup>49</sup> According to Broc Munro of Microsoft,  
4 “[w]e gravitate towards social platforms like LinkedIn to achieve more targeted marketing  
5 engagement. However, we know that our audiences don’t spend all their time on social media.  
6 LinkedIn Audience Network enables us to expand our reach to trusted sites while still respecting  
7 our audience targeting. This increases the impact of our advertising.”<sup>50</sup>

8           60. In July 2022, “LinkedIn Marketing Solutions surpassed \$5 billion in annual  
9 revenue[.]”<sup>51</sup> That figure is “expected to further grow to reach 10.35 billion U.S. dollars by  
10 2027.”<sup>52</sup>

11           61. According to LinkedIn, the LinkedIn Insight Tag, also called the Insight Tag is “[a]  
12 simple code snippet added to [a] website [that] can help you optimize your campaigns, retarget  
13 your website visitors, and learn more about your audiences.”<sup>53</sup> LinkedIn represents that the  
14 LinkedIn Insight Tag “enable[s] in-depth campaign reporting and unlock[s] valuable insights about  
15 your website visitors.”<sup>54</sup>

16           62. LinkedIn’s current iteration of its Insight Tag is a JavaScript-based code which  
17 allows for the installation of its software.<sup>55</sup> A critical feature allows the LinkedIn Insight Tag to  
18  
19

---

20 <sup>49</sup> LINKEDIN, ACCOUNT TARGETING, [https://business.linkedin.com/marketing-solutions/ad-](https://business.linkedin.com/marketing-solutions/ad-targeting)  
21 [targeting](https://business.linkedin.com/marketing-solutions/ad-targeting).

22 <sup>50</sup> LINKEDIN, LINKEDIN AUDIENCE NETWORK, [https://business.linkedin.com/marketing-](https://business.linkedin.com/marketing-solutions/native-advertising/linkedin-audience-network)  
23 [solutions/native-advertising/linkedin-audience-network](https://business.linkedin.com/marketing-solutions/native-advertising/linkedin-audience-network).

24 <sup>51</sup> *LinkedIn Business Highlights from Microsoft’s FY22 Q4 Earnings*, LINKEDIN PRESSROOM (July  
25 25, 2022), [https://news.linkedin.com/2022/july/linkedin-business-highlights-from-microsoft-s-](https://news.linkedin.com/2022/july/linkedin-business-highlights-from-microsoft-s-fy22-q4earnings#:~:text=And%20LinkedIn%20Marketing%20Solutions%20surpassed,revenue%20for%20the%20first%20time)  
26 [fy22-](https://news.linkedin.com/2022/july/linkedin-business-highlights-from-microsoft-s-fy22-q4earnings#:~:text=And%20LinkedIn%20Marketing%20Solutions%20surpassed,revenue%20for%20the%20first%20time)  
27 [q4earnings#:~:text=And%20LinkedIn%20Marketing%20Solutions%20surpassed,revenue%20for%20the%20first%20time](https://news.linkedin.com/2022/july/linkedin-business-highlights-from-microsoft-s-fy22-q4earnings#:~:text=And%20LinkedIn%20Marketing%20Solutions%20surpassed,revenue%20for%20the%20first%20time).

28 <sup>52</sup> Dencheva, *supra* note 34.

<sup>53</sup> LINKEDIN, INSIGHT TAG, <https://business.linkedin.com/marketing-solutions/insight-tag>.

<sup>54</sup> LINKEDIN, LINKEDIN INSIGHT TAG FAQs, <https://www.linkedin.com/help/lms/answer/a427660>.

<sup>55</sup> LINKEDIN, *supra* note 45.

1 track users, even when third-party cookies are blocked.<sup>56</sup> LinkedIn “recommend[s] using the  
2 JavaScript-based Insight Tag or Conversions API” because third-party cookie settings are being  
3 deprecated across the industry.<sup>57</sup> Embedding the JavaScript as a first-party cookie causes users’  
4 browsers to treat the LinkedIn Insight Tag as though it is offered by the website being visited,  
5 rather than by LinkedIn. Doing so ensures that the third-party cookie-blocking functions of  
6 modern web browsers do not prevent LinkedIn from collecting data through its Pixel.<sup>58</sup> Instead,  
7 the LinkedIn Pixel is shielded with the same privacy exemptions offered to first-party cookies.

8         63. When a user who has signed in to LinkedIn (even if the user subsequently logs out)  
9 is browsing a website where the LinkedIn Insight Tag has been embedded, an HTTP request is sent  
10 using cookies, which includes information about the user’s actions on the website.

11         64. These cookies also include data that differentiate users from one another and can be  
12 used to link the data collected to the user’s LinkedIn profile.

13         65. The HTTP request about an individual who has previously signed into LinkedIn  
14 includes requests from the “li\_sugr” and “lms\_ads” cookies. Each of these cookies are used by  
15 LinkedIn “to identify LinkedIn Members off LinkedIn” for advertising purposes.<sup>59</sup>

16         66. For example, the “li\_sugr” cookie is “[u]sed to make a probabilistic match of a  
17 user’s identity.”<sup>60</sup> Similarly, the “lms\_ads” cookie is “[u]sed to identify LinkedIn Members off  
18 LinkedIn for advertising.”<sup>61</sup>

19         67. A LinkedIn profile contains information including an individual’s first and last  
20 name, place of work, contact information, and other personal details. Based on information it  
21 obtains through the LinkedIn Pixel, Defendant LinkedIn is able to target its account holders for  
22 advertising.

---

23 <sup>56</sup> *Id.* (“It’s important for advertisers to prepare for these changes by switching to JavaScript tags  
24 and enabling ‘enhanced conversion tracking’ in the Insight Tag settings to continue capturing  
signals where 3rd party cookies are blocked.”).

25 <sup>57</sup> *See id.*

26 <sup>58</sup> *See id.*

27 <sup>59</sup> LINKEDIN, LINKEDIN COOKIE TABLE, <https://www.linkedin.com/legal/l/cookie-table>.

28 <sup>60</sup> *See id.*

<sup>61</sup> *See id.*

1           68.     LinkedIn never receives consent from users to intercept and collect electronic  
2 communications containing their sensitive and unlawfully-disclosed information. In fact, LinkedIn  
3 expressly warrants the opposite.

4           69.     When first signing up, a user agrees to the User Agreement.<sup>62</sup> By using or  
5 continuing to use LinkedIn's Services, users agree to two additional agreements: the Privacy  
6 Policy<sup>63</sup> and the Cookie Policy.<sup>64</sup> For California residents, LinkedIn also publishes a California  
7 Privacy Disclosure.<sup>65</sup>

8           70.     LinkedIn's Privacy Policy begins by stating that "LinkedIn's mission is to connect  
9 the world's professionals . . . . Central to this mission is our commitment to be transparent about  
10 the data we collect about you, how it is used and with whom it is shared."<sup>66</sup>

11          71.     The Privacy Policy goes on to describe what data LinkedIn collects from various  
12 sources, including cookies and similar technologies.<sup>67</sup> LinkedIn states "we use cookies and similar  
13 technologies (e.g., pixels and ad tags) to collect data (e.g., device IDs) to recognize you and your  
14 device(s) on, off and across different services and devices where you have engaged with our  
15 Services. We also allow some others to use cookies as described in our Cookie Policy."<sup>68</sup>

16          72.     However, LinkedIn offers an express representation: "**We will only collect and**  
17 **process personal data about you where we have lawful bases.**"<sup>69</sup>

18          73.     Despite this explicit representation, LinkedIn intentionally intercepts and receives  
19 sensitive and unlawfully disclosed information in violation of state and federal privacy laws.  
20  
21

---

22 <sup>62</sup> LINKEDIN, USER AGREEMENT, <https://www.linkedin.com/legal/user-agreement>.

23 <sup>63</sup> LINKEDIN, PRIVACY POLICY, <https://www.linkedin.com/legal/privacy-policy>.

24 <sup>64</sup> LINKEDIN, COOKIE POLICY, <https://www.linkedin.com/legal/cookie-policy>.

25 <sup>65</sup> LINKEDIN, CALIFORNIA PRIVACY DISCLOSURE, <https://www.linkedin.com/legal/california-privacy-disclosure>.

26 <sup>66</sup> LINKEDIN, PRIVACY POLICY, <https://www.linkedin.com/legal/privacy-policy>.

27 <sup>67</sup> *Id.*

28 <sup>68</sup> *Id.*

<sup>69</sup> *Id.* (emphasis added).

74. Users never choose to provide sensitive information to LinkedIn because, among other reasons, they never know whether a particular website uses the LinkedIn Insight Tag, and, if so, what sensitive personal data it collects.

**F. How Defendant Spring Fertility Disclosed Plaintiff's and Class Members' Protected Health Information and Assisted with Intercepting Communications**

75. Defendant Spring Fertility is a corporation that focuses on providing fertility services, such as in vitro fertilization ("IVF").

76. Spring Fertility owns and operates the [www.springfertility.com](http://www.springfertility.com) Website, where it encourages prospective patients to schedule consultations for its fertility services.

77. At all relevant times Defendant Spring Fertility's Website utilized the Facebook Tracking Pixel and LinkedIn Insight Tag.

78. Through the Facebook Tracking Pixel and LinkedIn Insight Tag, Defendant Spring Fertility shared its patients' identities and online activity, including information related to consumers seeking to procure fertility treatment, with two of the world's largest social media companies for targeted advertising purposes.

79. Defendant Spring Fertility allows and encourages consumers to book consultations for fertility treatment on its Website.

**Figure 1:**



80. Once a consumer clicks the "BOOK A CONSULT" link, they are brought to the following webpage to provide additional personal information to Defendant Spring Fertility.

**Figure 2:**

The screenshot shows a registration form for Spring Fertility. On the left is a vertical image of a modern office interior with the text "SPRING FERTILITY" overlaid. The form itself is on a blue background and is titled "Hello! Tell us a little about yourself:". It contains several input fields: "FIRST NAME\*" and "LAST NAME\*" (both with "Legal Name" as placeholder text), "LAST NAME AT BIRTH (IF DIFFERENT)", "DOB (MM/DD/YYYY)\*", "SEX ASSIGNED AT BIRTH\*" (with "Female" and "Male" buttons), "IN YOUR OWN WORDS, WHAT IS YOUR GENDER?" (a dropdown menu with "Make a selection"), "EMAIL\*", and "PHONE\*". Below these fields is a question: "Do you agree to receive SMS messages regarding important information about your upcoming appointment?" with "Yes" and "No" buttons. At the bottom, there is a progress bar with "MY INFO" highlighted and a green "NEXT" button.

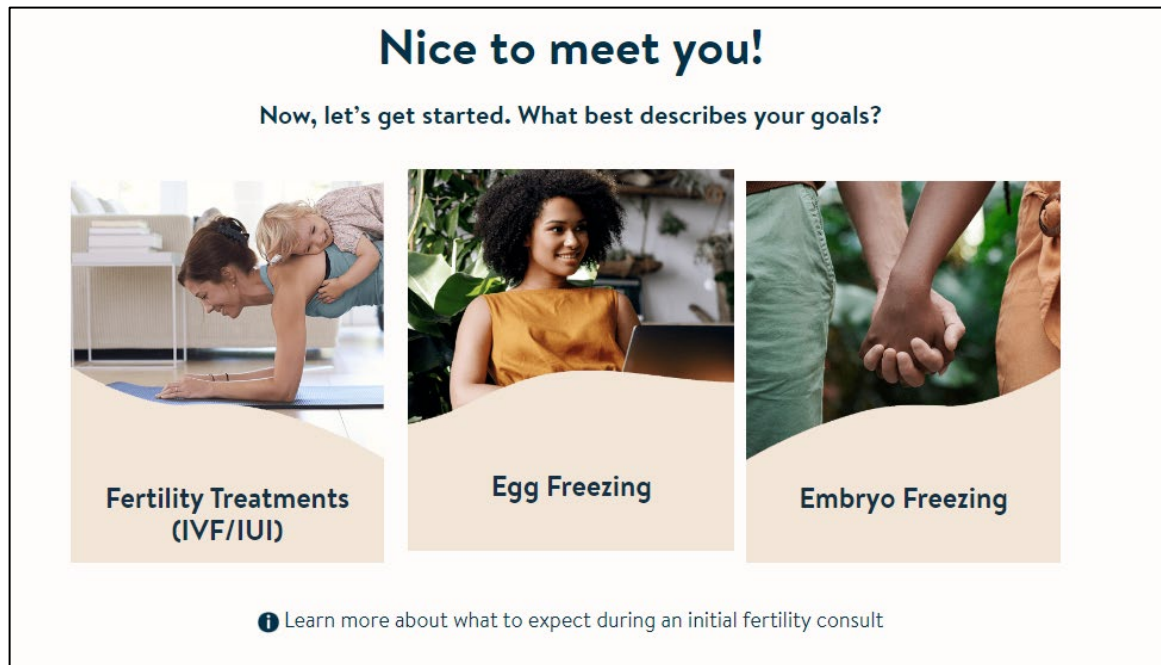
81. When a consumer fills out the requested information and clicks “NEXT,” they are taken to another webpage where Defendant Spring Fertility asks about the State they would like to receive services.

**Figure 3:**

The screenshot shows a webpage titled "Where are you interested in being seen?". It features three large, light-orange rectangular buttons arranged horizontally. Each button contains a circular icon with a map outline of a state: New York, California, and Oregon. Below each icon, the state name is written in orange text: "New York", "California", and "Oregon".

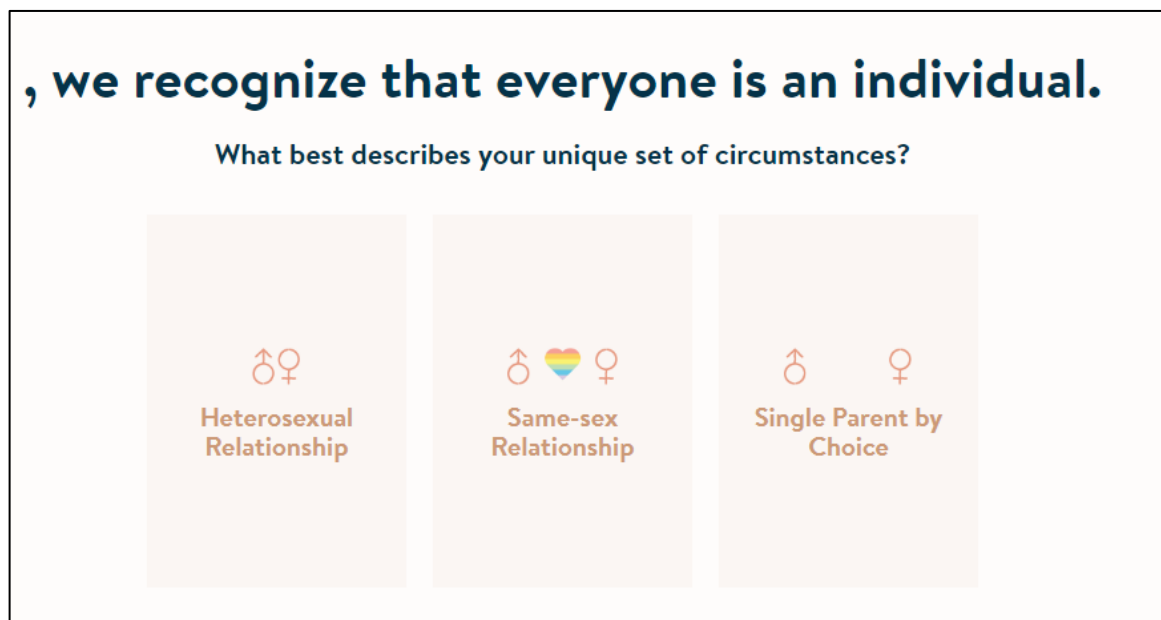
82. On the following page, consumers indicate the fertility services they are seeking treatment for.

**Figure 4:**



83. Next, Defendant Spring Fertility requests that consumers identify the type of relationship they are in, including whether they are in a “[s]ame-sex [r]elationship” or a “[s]ingle [p]arent by [c]hoice.”

**Figure 5:**



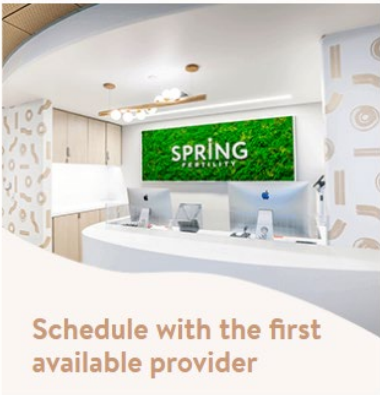
84. Defendant Spring Fertility next asks a host of questions related to a consumers preferred treatment location.

**Figures 6-8:**

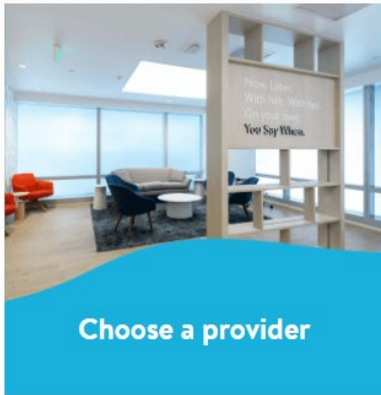
**Great! Which location is most convenient for you?**

San Francisco, Pac Heights	San Francisco, SOMA	Oakland
Danville	Sunnyvale	Redwood City

**Would you like to:**




**Schedule with the first available provider**




**Choose a provider**

**Would you prefer this appointment to be:**



**In-person**



**Via Teleconference**

Please note that if you complete your initial appointment virtually, your care team will schedule a follow-up appointment for your ultrasound and bloodwork. There is no difference in price between in-person and virtual consults.



85. Finally, Defendant Spring Fertility requests more personal information, including contact information, personal information related to a consumer’s partner, and insurance information.

**Figures 9-12:**

The screenshot shows a form titled "Just a few more things" with the following fields and options:

- ADDRESS\***: A text input field with a placeholder "0 of 255 max characters".
- ADDRESS 2**: A text input field with a placeholder "0 of 255 max characters".
- APARTMENT/SUITE NUMBER**: A text input field with a placeholder "0 of 255 max characters".
- CITY\***: A text input field with a placeholder "0 of 255 max characters".
- STATE\***: A dropdown menu with the text "Make a selection" and a downward arrow.
- ZIP\***: A text input field.
- DO YOU REQUIRE AN INTERPRETER?\***: Two radio button options, "YES" and "NO".

The screenshot shows a form titled "Just a few more things" with the following fields:

- PARTNER FIRST NAME\***: A text input field with a placeholder "Legal Name".
- PARTNER LAST NAME\***: A text input field with a placeholder "Legal Name".
- PARTNER LAST NAME AT BIRTH (IF DIFFERENT)**: A text input field.
- PARTNER DOB (MM/DD/YYYY)\***: A text input field.
- PARTNER EMAIL\***: A text input field.
- PARTNER PHONE\***: A text input field.

The screenshot shows a form titled "Just a few more things" with the following field and options:

- DO YOU HAVE FERTILITY-SPECIFIC INSURANCE?\***: Two radio button options, "Yes" and "No".

86. When a consumer enters Defendant Spring Fertility’s Website and begins the process of booking a fertility consultation, Defendant Spring Fertility transmitted the fact that the consumer was seeking to procure fertility treatment to Facebook and LinkedIn through the Facebook Tracking Pixel and LinkedIn Insight Tag.

87. For example, Defendant Spring Fertility incorporated the Facebook Tracking Pixel on its Website, allowing Defendant Facebook to intercept and record “PageView” and “SubscribedButtonClick” events, which detail information about which page on Defendant Spring Fertility’s Website the patient was viewing as well as the selections they were making.

88. Specifically, when booking a fertility consultation for IVF treatment, the PageView and SubscribedButtonClick event information shared with Facebook includes the terms “springfertility,” “book-a-consult,” and “IVF.” See Figures 13 and 14.

**Figures 13-14:**

```
Facebook
Endpoint:https://www.facebook.com
Data:
id 684212726404517
ev PageView
dl https://springfertility.com/book-a-consult-contact/?r=CA#gf_38
rl https://springfertility.com/book-a-consult/
```

```
Facebook
Endpoint:https://www.facebook.com
Data:
id 684212726404517
ev SubscribedButtonClick
dl https://springfertility.com/book-a-consult/location/?rel=H&int=IVF&r=CA&feid=40-255969#gf_40
rl https://springfertility.com/book-a-consult-goals/?r=CA&feid=39-255967
```

89. Each time Defendant Spring Fertility sent this activity data through the Facebook Tracking Pixel, it also disclosed a patient’s personally identifiable information, including their Facebook ID (“FID”). An FID is a unique and persistent identifier that Facebook assigns to each user. With it, any ordinary person can look up the user’s Facebook profile and name. Notably, while Facebook can easily identify any individual on its Facebook platform with only their unique FID, so too can any ordinary person who comes into possession of an FID. Facebook admits as much on its website. Indeed, ordinary persons who come into possession of the FID can connect to any Facebook profile.

90. A user who accessed Defendant Spring Fertility’s Website while logged into

1 Facebook transmitted what is known as a “c\_user cookie” to Facebook, which contained that user’s  
2 unencrypted FID.

3 91. When a visitor’s browser had recently logged out of an account, Facebook  
4 compelled the visitor’s browser to send a smaller set of cookies.

5 92. One such cookie was the “fr cookie” which contained, at least, an encrypted FID  
6 and browser identifier.<sup>70</sup> Facebook, at a minimum, used the fr cookie to identify users.<sup>71</sup>

7 93. If a visitor had never created an account, an even smaller set of cookies was  
8 transmitted.

9 94. At each stage, Defendant Spring Fertility also utilized the “\_fbp cookie,” which  
10 attached to a browser as a first-party cookie, and which Facebook used to identify a browser and a  
11 user.<sup>72</sup>

12 95. The c\_user cookie expires after 90 days if the user checked the “keep me logged in”  
13 checkbox on the website.<sup>73</sup> Otherwise, the c\_user cookie is cleared when the browser exits.<sup>74</sup>

14 96. The fr cookie expires after 90 days unless the visitor’s browser logs back into  
15 Facebook.<sup>75</sup> If that happens, the time resets, and another 90 days begins to accrue.<sup>76</sup>

16 97. The \_fbp cookie expires after 90 days unless the visitor’s browser accesses the same  
17 website.<sup>77</sup> If that happens, the time resets, and another 90 days begins to accrue.<sup>78</sup>

18 98. The Facebook Tracking Pixel used both first- and third-party cookies. A first-party  
19

---

20 <sup>70</sup> DATA PROTECTION COMMISSIONER, FACEBOOK IRELAND LTD, REPORT OF RE-AUDIT (Sept. 21,  
2012), [http://www.europe-v-facebook.org/ODPC\\_Review.pdf](http://www.europe-v-facebook.org/ODPC_Review.pdf).

21 <sup>71</sup> FACEBOOK, PRIVACY CENTER – COOKIES POLICY,  
22 <https://www.facebook.com/privacy/policies/cookies/?subpage=subpage-1.3>.

23 <sup>72</sup> *Id.*

24 <sup>73</sup> Seralthan, FACEBOOK COOKIES ANALYSIS (Mar. 14, 2019),  
<https://techexpertise.medium.com/facebook-cookies-analysis-e1cf6ffbf8a>.

25 <sup>74</sup> *Id.*

26 <sup>75</sup> *See id.*

27 <sup>76</sup> Confirmable through developer tools.

28 <sup>77</sup> FACEBOOK, PRIVACY CENTER – COOKIES POLICY,  
<https://mbasic.facebook.com/privacy/policies/cookies/printable/#annotation-1>.

<sup>78</sup> Also confirmable through developer tools.

1 cookie is “created by the website the user is visiting”—*i.e.*, Defendant Spring Fertility’s Website.<sup>79</sup>  
2 A third-party cookie is “created by a website with a domain name other than the one the user is  
3 currently visiting”—*i.e.*, Facebook.<sup>80</sup> The \_fbp cookie was always transmitted as a first-party  
4 cookie. A duplicate \_fbp cookie was sometimes sent as a third-party cookie, depending on whether  
5 the browser had recently logged into Facebook.

6 99. Facebook, at a minimum, used the fr, \_fbp, and c\_user cookies to link to FIDs and  
7 corresponding Facebook profiles. Defendant Spring Fertility sent these identifiers alongside the  
8 event data.

9 100. Plaintiff’s offsite activity report from her personal Facebook account confirms that  
10 her sensitive, confidential, and protected information was intercepted by Facebook through  
11 Defendant Spring Fertility’s Website.

12 101. Similar disclosures occurred through the LinkedIn Insight Tag.

13 102. For example, Defendant Spring Fertility incorporated the LinkedIn Insight Tag on  
14 its Website, allowing Defendant LinkedIn to intercept and record “CLICK” events, which detail  
15 information about which page on Defendant Spring Fertility’s Website the patient was viewing as  
16 well as the selections they were making.

17 103. Specifically, when booking a fertility consultation for IVF treatment, the CLICK  
18 event information shared with LinkedIn includes the terms “springfertility,” “book-a-consult,”  
19 “IVF.” *See* Figure 15.

20  
21  
22  
23  
24  
25  

---

26 <sup>79</sup> PC MAG, FIRST-PARTY COOKIE, <https://www.pcmag.com/encyclopedia/term/first-party-cookie>.  
This is confirmable by using developer tools to inspect a website’s cookies and track network  
27 activity.

28 <sup>80</sup> PC MAG, THIRD-PARTY COOKIE, <https://www.pcmag.com/encyclopedia/term/third-party-cookie>.  
This is also confirmable by tracking network activity.

**Figure 15:**

```
Data:
"signalType": "CLICK",
"href": "",
"domAttributes": {
  "elementSemanticType": null,
  "elementValue": null,
  "elementType": null,
  "tagName": "LABEL",
  "backgroundImageSrc": null,
  "imageSrc": null,
  "imageAlt": null,
  "innerText": "Oakland",
  "elementTitle": null,
  "cursor": "pointer",
  "formAction": "book-a-consult-location/?rel=H&int=IVF&r=CAfeid=40-255969#gf_41",
  "isFormSubmission": false
},

Cookies:
bcookie="v=2&ced8531e-1339-4214-87b5-b277dfa75233"
li_sugr=1a9e5b2f-a312-477a-8447-051e0b430241
liap=true
lms_ads=AQE Bcd0Y9yqMAAAAY7OTUXvuCi1gafK-
```

104. As shown in Figure 15, this interception also included the li\_sugr and lms\_ads cookies, which Defendant LinkedIn utilizes to identify its account holders for targeted advertising.

105. Plaintiff never consented, agreed, authorized, or otherwise permitted Defendant to disclose her PII and PHI. Plaintiff was never provided with any written notice that Defendant Spring Fertility disclosed the PII or PHI of users of the Website, nor was she provided any means of opting out of such disclosures. Defendant Spring Fertility nonetheless knowingly disclosed Plaintiff's PII and PHI, and assisted Facebook and LinkedIn in unlawfully intercepting this private information for targeted advertising purposes.

106. By law, Plaintiff is entitled to privacy in her protected health information and confidential communications. Defendant deprived Plaintiff of her privacy rights when it: (1) implemented a system that surreptitiously tracked, recorded, and disclosed Plaintiff's and other online patients' confidential communications, personally identifiable information, and protected health information; (2) disclosed and/or intercepted patients' protected health information; and (3) undertook this pattern of conduct without notifying Plaintiff and without obtaining her express

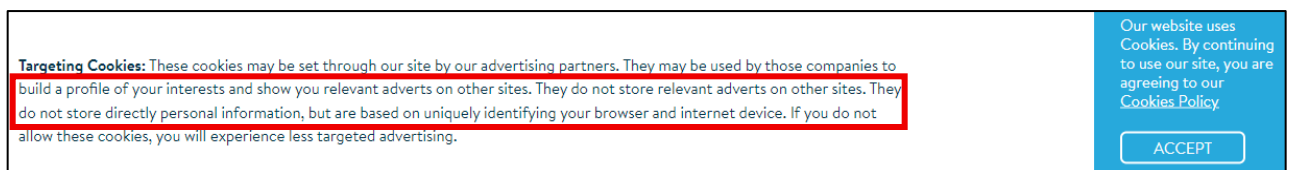
1 written consent. Plaintiff did not discover that Defendant disclosed and/or intercepted her  
2 personally identifiable information and protected health information, until around April 2024.

3 **G. Defendant Spring Fertility’s Cookie Banner Fails to Provide**  
4 **Notice to Consumers**

5 107. To the extent that consumers are aware of Defendant’s cookie banner, it is still  
6 grossly insufficient in notifying consumers of the types of information disclosed.

7 108. For example, Defendant Spring Fertility’s privacy policy expressly warrants that it  
8 will not assist a third party with intercepting communications that are paired with personally  
9 identifiable information.

10 **Figure 16:**



15 109. Both Facebook’s Tracking Pixel and LinkedIn’s Insight Tag are commonly known  
16 as a Targeting Cookies.<sup>81</sup>

17 110. As Figure 16 demonstrates, Defendant Spring Fertility expressly warrants that the  
18 “Targeting Cookies” on its Website “*do not store directly personal information*,” but are based on  
uniquely identifying your browser and internet device.” (emphasis added).

19 111. Based on this express representation, Defendant’s patients reasonably expect that  
20 any tracking that occurs on Defendant’s Website is done in an anonymized manner. In other  
21 words, while Defendant may represent that it builds advertising profiles, it also represents that such  
22 profiles will be maintained anonymously. However, Defendant violates its own representation.

23 112. As courts across the country have recognized the identifiers that the Facebook  
24 Tracking Pixel captures—Facebook ID, email address, first name, last name, and phone number—

25  
26 <sup>81</sup> <https://www.cookiepro.com/knowledge/what-are-targeting-advertising-cookies/#:~:text=Examples%20of%20targeting%20and%20advertising,them%20on%20social%20media%20platforms> (“Examples of targeting and advertising cookies include social media cookies that are placed on sites to track users around the web to provide ads to them on social media platforms.”).

1 constitute “directly personal information.” The same is true of the LinkedIn Insight Tag, based on  
2 the cookies it utilizes to identify its account holders. By assisting Facebook and LinkedIn with  
3 capturing this information anyway, Defendant Spring Fertility fails to receive consent from visitors  
4 to intercept their communications.

5 113. Additionally, consumers who do not interact with or click “Accept” on Defendant  
6 Spring Fertility’s cookie policy still have their sensitive and confidential information disclosed to  
7 Facebook and LinkedIn.

8 114. Even consumers that do click “Accept” would not understand that Defendant Spring  
9 Fertility is sharing confidential information about their fertility consultation appointments, *as this*  
10 *does not comply with the requirements of HIPAA and/or the CMIA for disclosing such*  
11 *information*, nor does it comply with the express representations in Spring Fertility’s own privacy  
12 policy.

13 115. For example, HIPAA requires that healthcare providers, like Defendant, receive a  
14 signed express authorization from the patient prior to the sharing of their protected health  
15 information, such as appointments related to fertility treatment. Defendant never received an  
16 express authorization from Plaintiff prior to sharing her protected health information related to her  
17 treatment for fertility services. Because Plaintiff never signed an express authorization to disclose  
18 such information she had no reason to believe that Defendant would be sharing her protected health  
19 information. Such conduct is illegal under state and federal law.

#### 20 **CLASS ACTION ALLEGATIONS**

21 116. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23  
22 individually and on behalf of the following Classes:

23 **Nationwide Class:** All natural persons in the United States who, during the class period,  
24 maintained a Facebook or LinkedIn account and booked a consultation on  
25 www.springfertility.com.

26 **California Class:** All natural persons in the State of California who, during the class  
27 period, maintained a Facebook or LinkedIn account and booked a consultation on  
28 www.springfertility.com.

1           117. Plaintiff reserves the right to modify the class definitions or add sub-classes as  
2 necessary prior to filing a motion for class certification.

3           118. The “Class Period” is the time period beginning on the date established by the  
4 Court’s determination of any applicable statute of limitations, after consideration of any tolling,  
5 concealment, and accrual issues, and ending on the date of entry of judgement.

6           119. Excluded from the Classes are Defendant; any affiliate, parent, or subsidiary of  
7 Defendant; any entity in which Defendant has a controlling interest; any officer, director, or  
8 employee of Defendant; any successor or assign of Defendant; anyone employed by counsel in this  
9 action; any judge to whom this case is assigned, his/her spouse and immediate family members;  
10 and members of the judge’s staff.

11           120. Numerosity. Members of the Classes are so numerous that joinder of all members is  
12 impracticable. The exact number of Class Members is unknown to Plaintiff at this time; however,  
13 it is estimated that there are at least thousands of individuals in the Classes. The identity of such  
14 membership is readily ascertainable from Defendant’s records and the records of third parties  
15 Facebook and LinkedIn.

16           121. Typicality. Plaintiff’s claims are typical of the claims of the Classes because  
17 Plaintiff used www.springfertility.com and had her personally identifiable information and  
18 protected health information disclosed to Facebook and LinkedIn without her express written  
19 authorization or knowledge. Plaintiff’s claims are based on the same legal theories as the claims of  
20 other Class members.

21           122. Adequacy. Plaintiff is prepared to take all necessary steps to represent fairly and  
22 adequately the interests of the Class Members. Plaintiff’s interests are coincident with, and not  
23 antagonistic to, those of the members of the Classes. Plaintiff is represented by attorneys with  
24 experience in the prosecution of class action litigation, generally, and in the emerging field of  
25 digital privacy litigation, specifically. Plaintiff’s attorneys are committed to vigorously  
26 prosecuting this action on behalf of the members of the Classes.

27           123. Commonality. Questions of law and fact common to the members of the Classes  
28 predominate over questions that may affect only individual members of the Classes because



1 Defendant has acted on grounds generally applicable to the Classes. Such generally applicable  
2 conduct is inherent in Defendant's wrongful conduct. Questions of law and fact common to the  
3 Classes include:

- 4 a. Whether Defendant intentionally tapped the lines of internet communication  
5 between patients and their fertility healthcare provider;
- 6 b. Whether Defendant's Website surreptitiously recorded personally identifiable  
7 information, protected health information, and related communications and  
8 subsequently, or simultaneously, disclosed that information to Facebook and  
9 LinkedIn;
- 10 c. Whether Facebook and LinkedIn are third-party eavesdroppers;
- 11 d. Whether Defendant's disclosures of personally identifiable information, protected  
12 health information, and related communications constituted an affirmative act of  
13 communication;
- 14 e. Whether Defendant's conduct, which allowed Facebook and LinkedIn—  
15 unauthorized persons—to view Plaintiff's and Class Members' personally  
16 identifiable information and protected health information, resulted in a breach of  
17 confidentiality;
- 18 f. Whether Defendant violated Plaintiff's and Class Members' privacy rights by using  
19 the Facebook Tracking Pixel and LinkedIn Insight Tag to record and communicate  
20 patients' confidential medical communications;
- 21 g. Whether Plaintiff and Class Members are entitled to damages under the ECPA, the  
22 CIPA, the CMIA, or any other relevant statute; and
- 23 h. Whether Defendant's actions violated Plaintiff's and Class Members' privacy rights  
24 as provided by the California Constitution.

25 124. Superiority. Class action treatment is the superior method for the fair and efficient  
26 adjudication of this controversy. Such treatment permits a large number of similarly situated  
27 persons to prosecute their common claims in a single forum simultaneously, efficiently, and  
28 without the unnecessary duplication of evidence, effort, or expense that numerous individual

1 actions would engender. The benefits of proceeding through the class mechanism, including  
2 providing injured persons or entities a method for obtaining redress on claims that could not  
3 practicably be pursued individually, substantially outweigh any potential difficulties in the  
4 management of this class action. Plaintiff knows of no special difficulty to be encountered in  
5 litigating this action that would preclude its maintenance as a class action.

6 **COUNT I**  
7 **Violation of the Electronic Communications Privacy Act,**  
8 **18 U.S.C. § 2511(1)**

9 125. Plaintiff repeats the allegations contained in the paragraphs above as if fully set  
10 forth herein and brings this count individually and on behalf of the members of the Nationwide  
11 Class against Defendant.

12 126. The Electronic Communications Privacy Act (“ECPA”) prohibits the intentional  
13 interception of the content of any electronic communication. 18 U.S.C. § 2511.

14 127. The ECPA protects both sending and the receipt of communications.

15 128. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or  
16 electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter  
17 119.

18 129. The transmission of Plaintiff’s private and confidential information to Defendant’s  
19 Website qualify as a “communication” under the ECPA’s definition of 18 U.S.C. § 2510(12).

20 130. The transmission of the private and confidential information between Plaintiff and  
21 Class Members and Defendant’s Website with which they chose to exchange communications are  
22 “transfer[s] of signs, signals, writing,...data, [and] intelligence of [some] nature transmitted in  
23 whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that  
24 affects interstate commerce” and are therefore “electronic communications” within the meaning of  
25 18 U.S.C. § 2510(12).

26 131. The ECPA defines “contents,” when used with respect to electronic  
27 communications, to “include[] any information concerning the substance, purport, or meaning of  
28 that communication.” 18 U.S.C. 18 U.S.C. § 2510(8).

132. The ECPA defines an interception as the “acquisition of the contents of any wire,

1 electronic, or oral communication through the use of any electronic, mechanical, or other device.”  
2 18 U.S.C. § 2510(4).

3 133. The ECPA defines “electronic, mechanical, or other device,” as “any  
4 device...which can be used to intercept a[n]...electronic communication[.]” 18 U.S.C. § 2510(5).

5 134. The following instruments constitute “devices” within the meaning of the ECPA:

- 6 a. The computer codes and programs Facebook and LinkedIn used to track Plaintiff
- 7 and Class Members communications while they were navigating the Website;
- 8 b. Plaintiff’s and Class Members’ browsers;
- 9 c. Plaintiff’s and Class Members’ mobile devices;
- 10 d. Defendant’s web and ad servers;
- 11 e. The plan Defendant, Facebook, and LinkedIn carried out to effectuate the tracking
- 12 and interception of Plaintiff’s and Class Members’ communications while they were
- 13 using a web browser to navigate the Website.

14 135. Plaintiff and Class Members’ interactions with Defendant’s Website are electronic  
15 communications under the ECPA.

16 136. By utilizing and embedding the Facebook Tracking Pixel and LinkedIn Insight Tag  
17 on its Website, Defendant intentionally intercepted, endeavored to intercept, and/or procured  
18 another person to intercept, the electronic communications of Plaintiff and Class Members in  
19 violation of 18 U.S.C. § 2511(1)(a).

20 137. Specifically, Defendant intercepted Plaintiff’s and Class Members’ electronic  
21 communications through the Facebook Tracking Pixel and LinkedIn Insight Tag, which tracked,  
22 stored and unlawfully disclosed Plaintiff’s and Class Members’ private and confidential  
23 information to third parties, such as Facebook and LinkedIn.

24 138. Defendant intercepted or assisted in the interception of communications that  
25 include, but are not necessarily limited to, communications to/from Plaintiff and Class Members  
26 regarding private and confidential information, including their Facebook ID, LinkedIn account and  
27 treatment information. This confidential information was then monetized for targeted advertising  
28 purposes.

1           139. By intentionally disclosing or endeavoring to disclose Plaintiff's and Class  
2 Members' electronic communications to affiliates and other third parties, while knowing or having  
3 reason to know that the information was obtained through the interception of an electronic  
4 communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

5           140. By intentionally using, or endeavoring to use, the contents of Plaintiff's and Class  
6 Members' electronic communications, while knowing or having reason to know that the  
7 information was obtained through the interception of an electronic communication in violation of  
8 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

9           141. Defendant intentionally intercepted or intentionally assisted in the interception of  
10 the contents of Plaintiff's and Class Members' electronic communications for the purpose of  
11 committing a criminal or tortious act in violation of the Constitution or laws of the United States or  
12 of any state, namely, invasion of privacy, among others.

13           142. The party exception in 18 U.S.C. § 2511(2)(d) does not permit a party that  
14 intercepts or causes interception to escape liability if the communication is intercepted for the  
15 purpose of committing any tortious or criminal act in violation of the Constitution or laws of the  
16 United States or of any State. Here, as alleged above, Defendant violated a provision of the Health  
17 Insurance Portability and Accountability Act, specifically 42 U.S.C. § 1320d-6(a)(3). This  
18 provision imposes a criminal penalty for knowingly disclosing individually identifiable health  
19 information ("IIHI") to a third party. HIPAA defines IIHI as:

20           any information, including demographic information collected from  
21 an individual, that—(A) is created or received by a health care  
22 provider ... (B) relates to the past, present, or future physical or  
23 mental health or condition of an individual, the provision of health  
24 care to an individual, or the past, present, or future payment for the  
provision of health care to an individual, and (i) identifies the  
individual; or (ii) with respect to which there is a reasonable basis to  
believe that the information can be used to identify the individual.<sup>82</sup>

25           143. Plaintiff's information that Defendant intercepted and disclosed to Facebook and  
26 LinkedIn qualifies as IIHI, and Defendant violated Plaintiff's and Class Members' expectations of  
27 privacy. Such conduct constitutes tortious and/or criminal conduct through a violation of 42

28  

---

<sup>82</sup> 42 U.S.C. § 1320d-6.

1 U.S.C. § 1320d-6. Defendant used the wire or electronic communications to increase its profit  
2 margins. Defendant specifically used the Facebook Tracking Pixel and LinkedIn Insight Tag to  
3 track and utilize Plaintiff's and Class Members' private and confidential information for financial  
4 gain.

5 144. Defendant was not acting under the color of law to intercept Plaintiff's and Class  
6 Members' wire or electronic communications.

7 145. Plaintiff and Class Members did not authorize Defendant to acquire the content of  
8 their communications for purposes of invading Plaintiff's and Class Members' privacy through the  
9 Facebook Tracking Pixel or LinkedIn Insight Tag. Plaintiff and Class Members had a reasonable  
10 expectation that Defendant would not intercept or assist in the interception of their private and  
11 confidential information without their knowledge or consent.

12 146. The foregoing acts and omission therefore constitute numerous violations of 18  
13 U.S.C. § 2511(1), *et seq.*

14 147. As a result of each and every violation thereof, on behalf of herself and the Class,  
15 Plaintiff seeks statutory damages of \$10,000 or \$100 per day for each violation of 18 U.S.C. §  
16 2510, *et seq.* under 18 U.S.C. § 2520.

17 **COUNT II**  
18 **Violation of the California Confidentiality of Medical Information Act,**  
19 **Cal. Civ. Code § 56.10**

20 148. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set  
21 forth herein and brings this claim individually and on behalf of the proposed California Class  
22 against Defendant.

23 149. Under the California Confidentiality of Medical Information Act (the "CMIA"),  
24 California Civil Code Section 56.10, providers of health care are prohibited from disclosing  
25 medical information relating to their patients without a patient's authorization. Medical  
26 information refers to:

27 any individually identifiable information, in electronic or physical  
28 form, in possession of or derived from a provider of health care . . .  
regarding a patient's medical history . . . reproductive or sexual health  
application information, mental or physical condition, or treatment.  
'Individually Identifiable' means that the medical information

1 includes or contains any element of personal identifying information  
2 sufficient to allow identification of the individual . . . .<sup>83</sup>

3 150. Plaintiff and Class Members are patients under the definition of the CMIA because  
4 Plaintiff and Class Members received “health care services from a provider of health care” and the  
5 information Spring Fertility shared to Facebook and LinkedIn was “medical information  
6 pertain[ing]” to Plaintiff and Class Members. Cal. Civ. Code § 56.05(m).

7 151. Defendant Spring Fertility is a “provider of health care” as defined in CMIA section  
8 56.05(p) because it offers fertility services. Defendant Spring Fertility is also considered a  
9 “provider of health care” under the CMIA because its Website maintains medical information and  
10 offers software to consumers that is designed to maintain medical information for the purposes of  
11 allowing its users to manage their information or make the information available to a health care  
12 provider, or for the diagnosis, treatment, or management of a medical condition. Cal. Civ. Code §  
13 56.06(a)–(b).

14 152. Therefore, as a provider of health care, Defendant Spring Fertility is subject to the  
15 requirements of the CMIA and had an ongoing obligation to comply with the CMIA’s requirements  
16 regarding the maintenance of its user’s medical information.

17 153. As set forth above, a Facebook ID is an identifier sufficient to allow identification  
18 of an individual. Along with patients’ Facebook ID, Spring Fertility disclosed to Facebook several  
19 pieces of information regarding its patients’ use of the Spring Fertility Website, which included,  
20 but was not limited to: treatments patients were seeking, such as booking consultations for fertility  
21 services.

22 154. Similarly, as set forth above, the li\_sugr and lms\_ads cookies allow LinkedIn to  
23 identify its individual account holders. Through these cookies, Spring Fertility disclosed to  
24 LinkedIn several pieces of information regarding its patients’ of the Spring Fertility Wesbite,  
25 which included, but was not limited to: treatments patients were seeking, such as booking  
26 consultations for fertility services.

27 155. This patient information was derived from a provider of health care regarding

28 

---

<sup>83</sup> Cal. Civ. Code § 56.05(j).

1 patients' medical treatment and physical condition. Accordingly, it constituted medical  
2 information pursuant to the CMIA.

3 156. As demonstrated above, Defendant Spring Fertility failed to obtain its patients' valid  
4 authorization for the disclosure of medical information.

5 157. A valid authorization for disclosure of medical information must: (1) be "clearly  
6 separate from any other language present on the same page and is executed by a signature that  
7 serves no other purpose than to execute the authorization"; (2) be signed and dated by the patient or  
8 her representative; (3) state the name and function of the third party that receives the information;  
9 and (4) state a specific date after which the authorization expires. Cal. Civ. Code § 56.11(b).

10 Accordingly, any information set forth in Defendant's Website Privacy Policy does not qualify as a  
11 valid authorization.

12 158. Based on the above, Defendant Spring Fertility violated the CMIA by disclosing its  
13 patients' medical information with Facebook and LinkedIn, along with information sufficient to  
14 identify each individual patient.

15 159. Under the CMIA, a patient may recover compensatory damages, punitive damages  
16 not to exceed \$3,000 dollars, attorneys' fees not to exceed \$1,000, and the costs of litigation for  
17 any violating disclosure of medical information. Cal. Civ. Code § 56.35. Alternatively, a patient  
18 may recover nominal damages of \$1,000 for any negligent release of medical information. Cal.  
19 Civ. Code § 56.36.

20 **COUNT III**  
21 **Violation of the California Invasion of Privacy Act,**  
22 **Cal. Penal Code § 631**

23 160. Plaintiff repeats the allegations contained in the paragraphs above as if fully set  
24 forth herein and brings this count individually and on behalf of the members of the California Class  
25 against Defendant.

26 161. The California Invasion of Privacy Act (the "CIPA") is codified at California Penal  
27 Code Sections 630 to 638. The CIPA begins with its statement of purpose—namely, that the  
28 purpose of the CIPA is to "protect the right of privacy of the people of [California]" from the threat  
posed by "advances in science and technology [that] have led to the development of new devices

1 and techniques for the purpose of eavesdropping upon private communications . . .” Cal. Penal  
2 Code § 630.

3 162. A person violates California Penal Code Section 631(a), if:  
4 by means of any machine, instrument, or contrivance, or in any other  
5 manner, [s/he] intentionally taps, or makes any unauthorized  
6 connection, whether physically, electrically, acoustically, inductively,  
7 or otherwise, with any telegraph or telephone wire, line, cable, or  
8 instrument, including the wire, line, cable, or instrument of any  
9 internal telephonic communication system, or [s/he] willfully and  
10 without the consent of all parties to the communication, or in any  
11 unauthorized manner, reads, or attempts to read, or to learn the  
12 contents or meaning of any message, report, or communication while  
13 the same is in transit or passing over any wire, line, or cable, or is being  
14 sent from, or received at any place within this state; or [s/he] uses, or  
15 attempts to use, in any manner, or for any purpose, or to communicate  
16 in any way, any information so obtained . . .<sup>84</sup>

17 163. Further, a person violates section 631(a) if s/he “aids, agrees with, employs, or  
18 conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts  
19 or things mentioned” in the preceding paragraph. *Id.*

20 164. To avoid liability under section 631(a), a defendant must show it had the consent of  
21 all parties to a communication.

22 165. At all relevant times, Spring Fertility aided, agreed with, and conspired with Facebook  
23 and LinkedIn to track and intercept Plaintiff’s and Class Members’ internet communications while  
24 using www.springfertility.com to book fertility consultations. These communications were  
25 intercepted without the authorization and consent of Plaintiff and Class Members.

26 166. Spring Fertility, while aiding and assisting Facebook and LinkedIn’s wiretapping,  
27 intended to help Facebook and LinkedIn learn some meaning of the content in the URLs and the  
28 content the visitors requested.

167. The following items constitute “machine[s], instrument[s], or contrivance[s]” under  
the CIPA, and even if they do not, the Facebook Tracking Pixel and LinkedIn Insight Tag fall under  
the broad catch-all category of “any other manner”:

a. The computer codes and programs Defendant, Facebook and LinkedIn used to track

---

<sup>84</sup> Cal. Penal Code § 631(a).



1 Plaintiff and Class Members' communications while they were navigating  
2 www.springfertility.com;

- 3 b. Plaintiff's and Class Members' browsers;
- 4 c. Plaintiff's and Class Members' computing and mobile devices;
- 5 d. Defendant's, Facebook's and LinkedIn's web and ad servers;
- 6 e. The web and ad servers from which Defendant, Facebook and LinkedIn tracked and  
7 intercepted Plaintiff's and Class Members' communications while they were using a  
8 web browser to access or navigate www.springfertility.com;
- 9 f. The computer codes and programs used by Defendant, Facebook and LinkedIn to  
10 effectuate the tracking and interception of Plaintiff's and Class Members'  
11 communications while they were using a browser to visit www.springfertility.com;  
12 and
- 13 g. The plan Defendant, Facebook and LinkedIn carried out to effectuate the tracking  
14 and interception of Plaintiff's and Class Members' communications while they were  
15 using a web browser or mobile device to visit www.springfertility.com.

16 168. At all relevant times, Facebook and LinkedIn, though the Facebook Tracking Pixel  
17 and LinkedIn Insight Tag, intentionally tapped or made unauthorized connections with, the lines of  
18 internet communications between Plaintiff and Class Members and Spring Fertility's Website  
19 without the consent of all parties to the communication.

20 169. Facebook and LinkedIn, willfully and without the consent of Plaintiff and Class  
21 Members, read or attempted to read, or learn the contents or meaning of Plaintiff's and Class  
22 Members' communications to Spring Fertility while the communications are in transit or passing  
23 over any wire, line or able, or were being received at any place within California when it  
24 intercepted Plaintiff's and Class Members' communications and data with Spring Fertility.

25 170. Facebook and LinkedIn used or attempted to use the communications and  
26 information they received through their tracking technology, including to supply advertising  
27 services.

28 171. By incorporating the Facebook Tracking Pixel and LinkedIn Insight Tag onto the

1 Website, Spring Fertility aided, agreed with, employed, and conspired with Facebook and LinkedIn  
2 to carry out the wrongful conduct alleged herein.

3 172. The patient communication information that Spring Fertility transmitted using the  
4 Facebook Tracking Pixel and LinkedIn Insight Tag, such as fertility consultation booking  
5 information, constituted protected health information.

6 173. As a result of the above violations, Defendant is liable to Plaintiff and other Class  
7 Members in the amount of \$5,000 dollars per violation or three times the amount of actual  
8 damages, whichever is greater. Additionally, California Penal Code Section 637.2 specifically  
9 states that “[it] is not a necessary prerequisite to an action pursuant to this section that the plaintiff  
10 has suffered, or be threatened with, actual damages.”

11 174. Under the CIPA, Defendant is also liable for reasonable attorney’s fees, and other  
12 litigation costs, injunctive and declaratory relief, and punitive damages in an amount to be  
13 determined by a jury, but sufficient to prevent the same or similar conduct by Defendant in the  
14 future.

15 **COUNT IV**  
16 **Violation of the California Invasion of Privacy Act,**  
17 **Cal. Penal Code § 632**

18 175. Plaintiff repeats the allegations contained in the paragraphs above as if fully set  
19 forth herein and brings this count individually and on behalf of the members of the California Class  
20 against Defendant.

21 176. Cal. Penal Code § 632 prohibits “intentionally and without the consent of all parties  
22 to a confidential communication,” the “use[] [of] an electronic amplifying or recording device to  
23 eavesdrop upon or record the confidential communication.”

24 177. Section 632 defines “confidential communication” as “any communication carried  
25 on in circumstances as may reasonably indicate that any party to the communication desires it to be  
26 confined to the parties thereto[.]”

27 178. Plaintiff’s and Class members’ communications to Spring Fertility, including their  
28 sensitive personal and health information, such as their fertility treatments and sexual orientation,  
were confidential communications for purposes of § 632, because Plaintiff and Class Members had

1 an objectively reasonable expectation of privacy in this data.

2 179. Plaintiff and Class Members expected their communications to Spring Fertility to be  
3 confined to Spring Fertility in part, because of Spring Fertility's representations that these  
4 communications would remain confidential as well as the legal protections afforded to such  
5 information. Plaintiff and Class Members did not expect third parties, and specifically Facebook  
6 and LinkedIn, to secretly eavesdrop upon or record this information and their communications.

7 180. Facebook and LinkedIn's tracking technology, i.e., the Facebook Tracking Pixel and  
8 LinkedIn Insight Tag, are all electronic amplifying or recording devices for purposes of § 632.

9 181. By contemporaneously intercepting and recording Plaintiff's and Class Members'  
10 confidential communications to Spring Fertility through this technology, Facebook and LinkedIn  
11 eavesdropped and/or recorded confidential communications through an electronic amplifying or  
12 recording device in violation of § 632 of CIPA.

13 182. At no time did Plaintiff or Class Members consent to Facebook and LinkedIn's  
14 conduct, nor could they reasonably expect that their communications to Spring Fertility would be  
15 overheard or recorded by Facebook and LinkedIn.

16 183. Facebook and LinkedIn utilized Plaintiff's and Class Members' sensitive personal  
17 and health information for their own purposes, including for targeted advertising.

18 184. Plaintiff and Class Members seek statutory damages in accordance with § 637.2(a)  
19 which provides for the greater of: (1) \$5,000 per violation; or (2) three times the amount of  
20 damages sustained by Plaintiff and the Classes in an amount to be proven at trial, as well as  
21 injunctive or other equitable relief.

22 185. Plaintiff and Class Members have also suffered irreparable injury from these  
23 unauthorized acts. Plaintiff's and Class Members' sensitive data has been collected, viewed,  
24 accessed, stored, by Facebook and LinkedIn, have not been destroyed, and due to the continuing  
25 threat of such injury, have no adequate remedy at law. Plaintiff and Class Members are  
26 accordingly entitled to injunctive relief.

**COUNT V**  
**Invasion of Privacy Under California's Constitution**

186. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein and brings this count individually and on behalf of the members of the California Class against Defendant.

187. Plaintiff and Class Members have an interest in: (1) precluding the dissemination and/or misuse of their sensitive, confidential communications and protected health information; and (2) making personal decisions and/or conducting personal activities without observation, intrusion, or interference, including, but not limited to, the right to visit and interact with various internet sites without being subjected to wiretaps without Plaintiff's and Class Members' knowledge or consent.

188. At all relevant times, by using the Facebook Tracking Pixel and LinkedIn Insight Tag to record and communicate patients' personal identifiers alongside their confidential medical communications, Defendant intentionally invaded Plaintiff's and Class Members' privacy rights under the California Constitution.

189. Plaintiff and Class Members had a reasonable expectation that their communications, identities, health information, and other data would remain confidential, and that Defendant would not install wiretaps on [www.springfertility.com](http://www.springfertility.com).

190. Plaintiff and Class Members did not authorize Defendant to record and transmit Plaintiff's and Class Members' private medical communications alongside their personally identifiable and health information.

191. This invasion of privacy was serious in nature, scope, and impact because it related to patients' private medical communications. Moreover, it constituted an egregious breach of the societal norms underlying the privacy right.

192. Accordingly, Plaintiff and Class Members seek all relief available for invasion of privacy under the California Constitution.

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiff prays for relief and judgment, as follows:

- 1 a. For a determination that this action is a proper class action;
- 2 b. For an order certifying the Classes, naming Plaintiff as representative of the
- 3 Classes, and naming Plaintiff's attorneys as Class Counsel to represent the
- 4 Classes;
- 5 c. For an order declaring that Defendant's conduct violated the statutes
- 6 referenced herein;
- 7 d. For an order finding in favor of Plaintiff and the Classes on all counts
- 8 asserted herein;
- 9 e. For an award of compensatory damages, including statutory damages where
- 10 available, to Plaintiff and the Class Members against Defendant for all
- 11 damages sustained as a result of Defendant's wrongdoing, in an amount to
- 12 be proven at trial;
- 13 f. For punitive damages, as warranted, in an amount to be determined at trial;
- 14 g. For an order requiring Defendant to disgorge revenues and profits
- 15 wrongfully obtained;
- 16 h. For prejudgment interest on all amounts awarded;
- 17 i. For injunctive relief as pleaded or as the Court may deem proper;
- 18 j. For an order awarding Plaintiff and the Classes their reasonable attorneys'
- 19 fees and expenses and costs of suit; and
- 20 k. For an order granting Plaintiff and Class Members such further relief as the
- 21 Court deems appropriate.

22 **DEMAND FOR JURY TRIAL**

23 Plaintiff on behalf of herself and the proposed Classes demands a trial by jury for all of the

24 claims asserted in this Complaint so triable.

25 Dated: November 5, 2025

Respectfully submitted,

26 **BURSOR & FISHER, P.A.**

27 By: /s/ Sarah N. Westcot

28

Sarah N. Westcot

Sarah N. Westcot (State Bar No. 264916)  
701 Brickell Ave., Suite 2100  
Miami, FL 33131-2800  
Telephone: (305) 330-5512  
Facsimile: (305) 676-9006  
Email: swestcot@bursor.com

*Counsel for Plaintiff*